

ALSD Local 106 (Rev. 07/13) Application for a Search Warrant

# UNITED STATES DISTRICT COURT

for the  
Southern District of Alabama

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

information associated with [REDACTED] that is stored  
at premises controlled by T-Mobile

23-MJ-194-B  
Case No. 23-CR-149/23-MJ-156

Filed Under Seal

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
See Attachment A (incorporated by reference).

located in the \_\_\_\_\_ District of \_\_\_\_\_ New Jersey \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):  
See Attachment B (incorporated by reference).

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

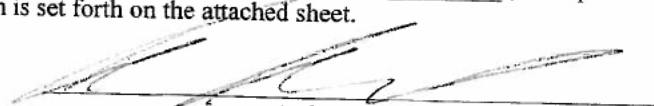
The search is related to a violation of:

Code Section  
18 U.S.C. §§ 1349, 1344, 513  
(a), 2314, and 1028A

Offense Description  
Fraud conspiracy, bank fraud, possession of counterfeited or forged securities, interstate transportation of counterfeited or forged securities, and aggravated identity theft

The application is based on these facts:  
See attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


  
Applicant's signature

Daniel Wessel, U.S. Postal Inspector

Printed name and title

Sworn to before me and attestation acknowledged pursuant to FRCP 4.1(b)(2).

Date: August 11, 2023

  
Judge's signature

City and state: Mobile, Alabama

Sonja F. Bivins, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF ALABAMA

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
[REDACTED] THAT IS STORED AT  
PREMISES CONTROLLED BY T-  
MOBILE

Case No. 23-CR-149-WS

Case No. 23-MJ-156-N

23-MJ-144-B

Filed Under Seal

AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT

I, Daniel Wessel, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by T-Mobile, a wireless provider headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require T-Mobile to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Postal Inspector assigned to the United States Postal Inspection Service's ("USPIS") Mobile, Alabama Domicile. In this capacity, I am responsible for investigating criminal activity related to the United States Postal Service in Mississippi and Alabama. I have been a Postal Inspector since April 2021. Prior to becoming a Postal Inspector, I was employed as a Special Agent with the United States Naval Criminal Investigative Service since September 2015. I have received training at the Federal Law Enforcement Training Center in criminal investigations and financial crimes. I have a certificate in Forensic Accounting from Georgetown University and have

been a Certified Fraud Examiner since 2012. In the course of my training and experience, I have worked on numerous investigations involving fraud. Pursuant to my duties as a Postal Inspector, I have gained experience in investigations of bank fraud pertaining to the theft and counterfeiting of checks. I have participated in search and seizure operations dealing with these types of criminal offenses. I have previously written, and served, and search warrants for multiple cell phones. I have also reviewed the contents of the contents of numerous cell phones after obtaining the contents via a search warrant related to altered and counterfeit checks. I have previously sworn, executed, and reviewed search warrants for location data pertaining to cellphones.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. All dates, times, amounts, and locations referenced in my affidavit are approximations.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1349 (fraud conspiracy), 1344 (bank fraud), 513(a) (possession of counterfeited or forged securities), 2314 (interstate transportation of counterfeited or forged securities), and 1028A (aggravated identity theft) have been committed by

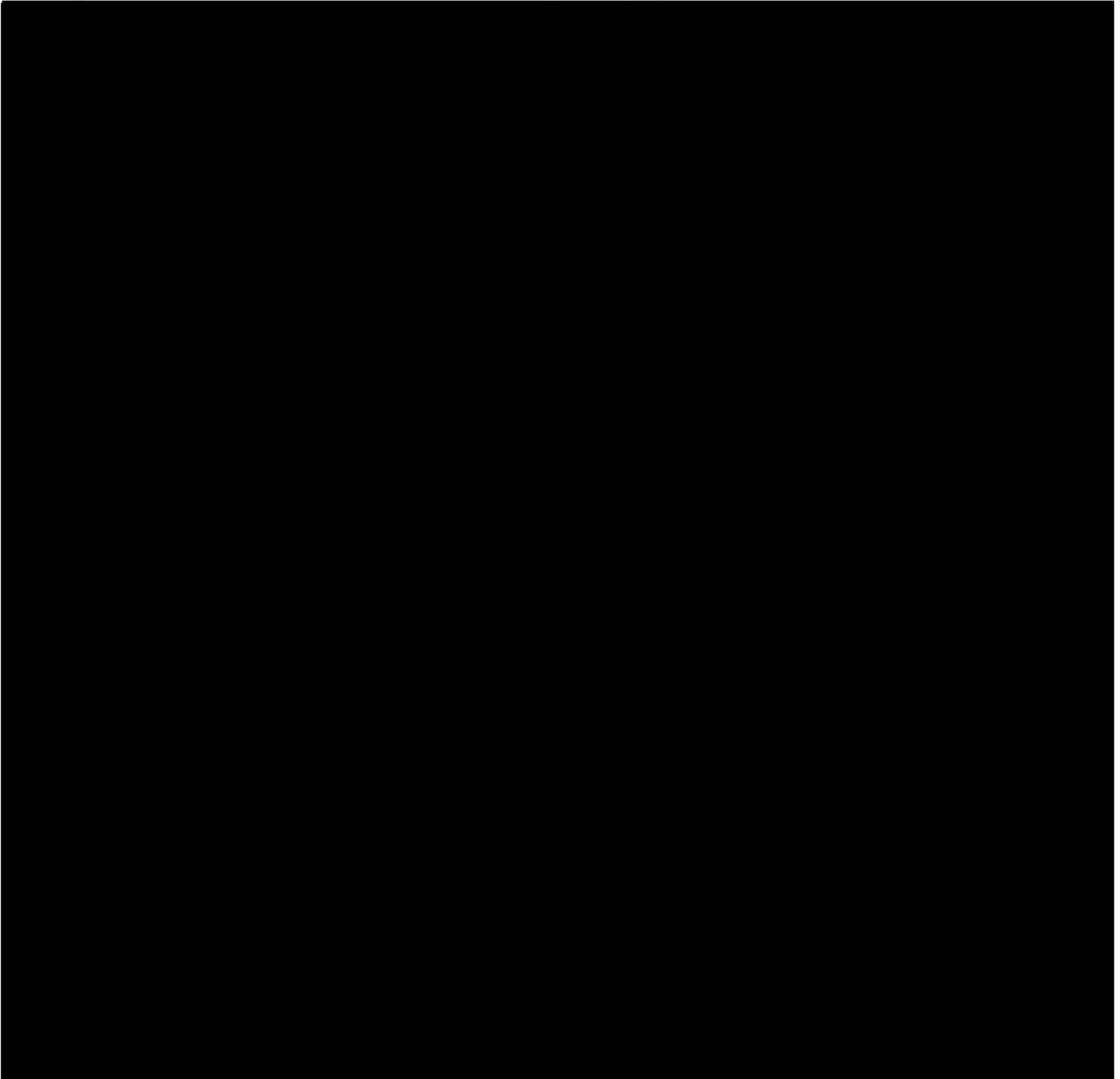
[REDACTED], and others, both known and unknown. There is also probable cause to search the information described in Attachment A and for evidence, instrumentalities, contraband, or fruits of these crimes, as further described in Attachment B.

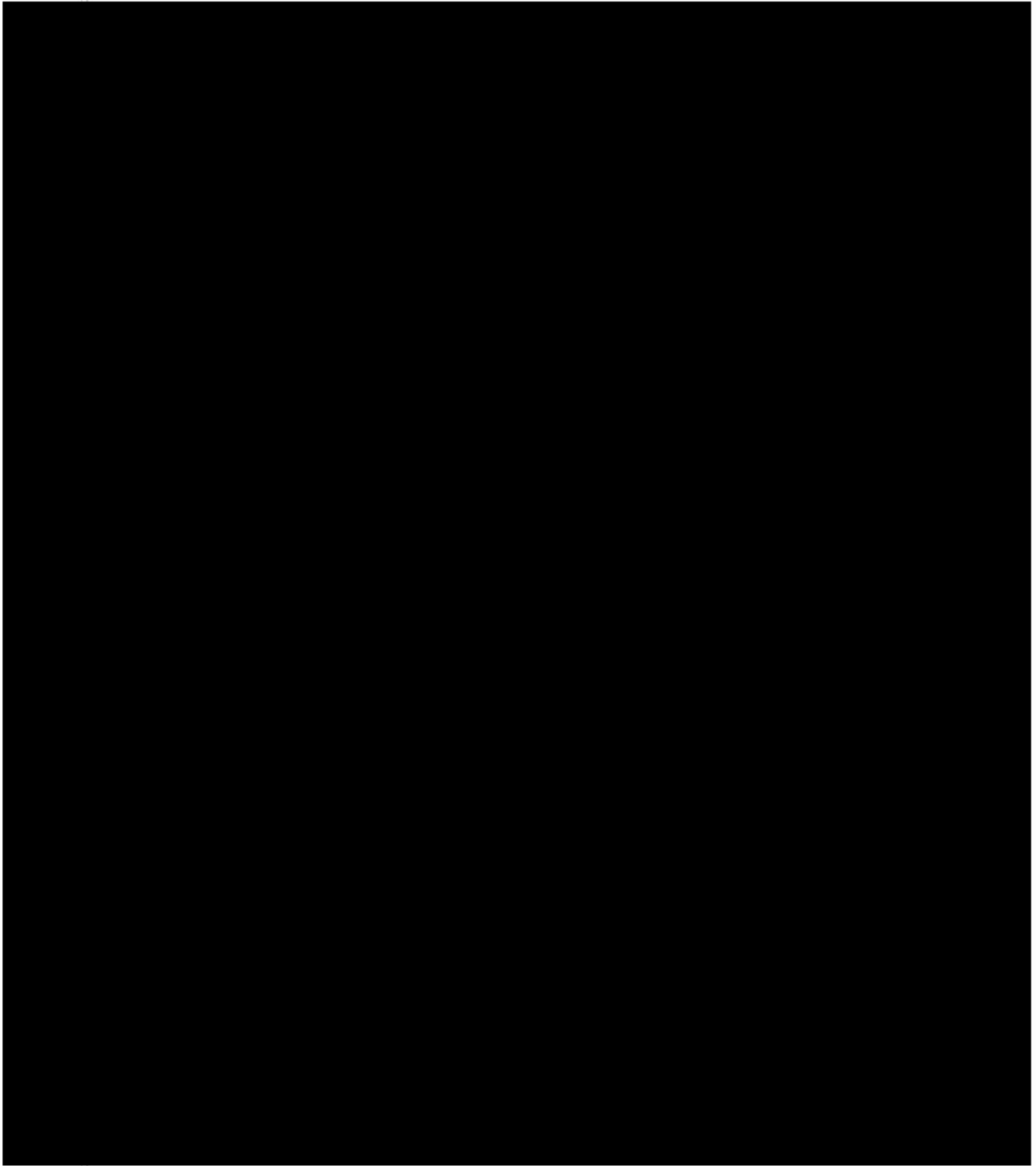
#### **JURISDICTION**

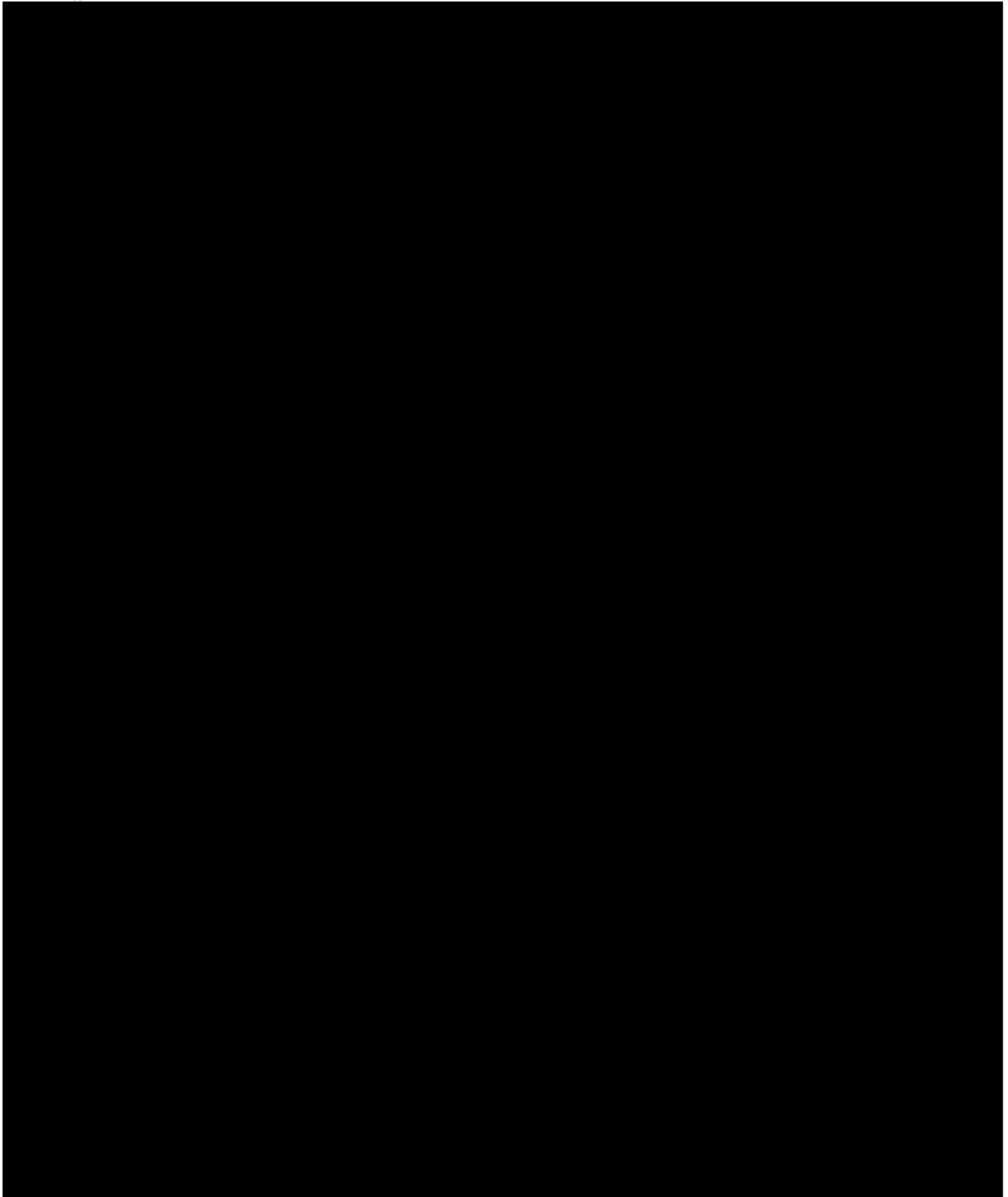
5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

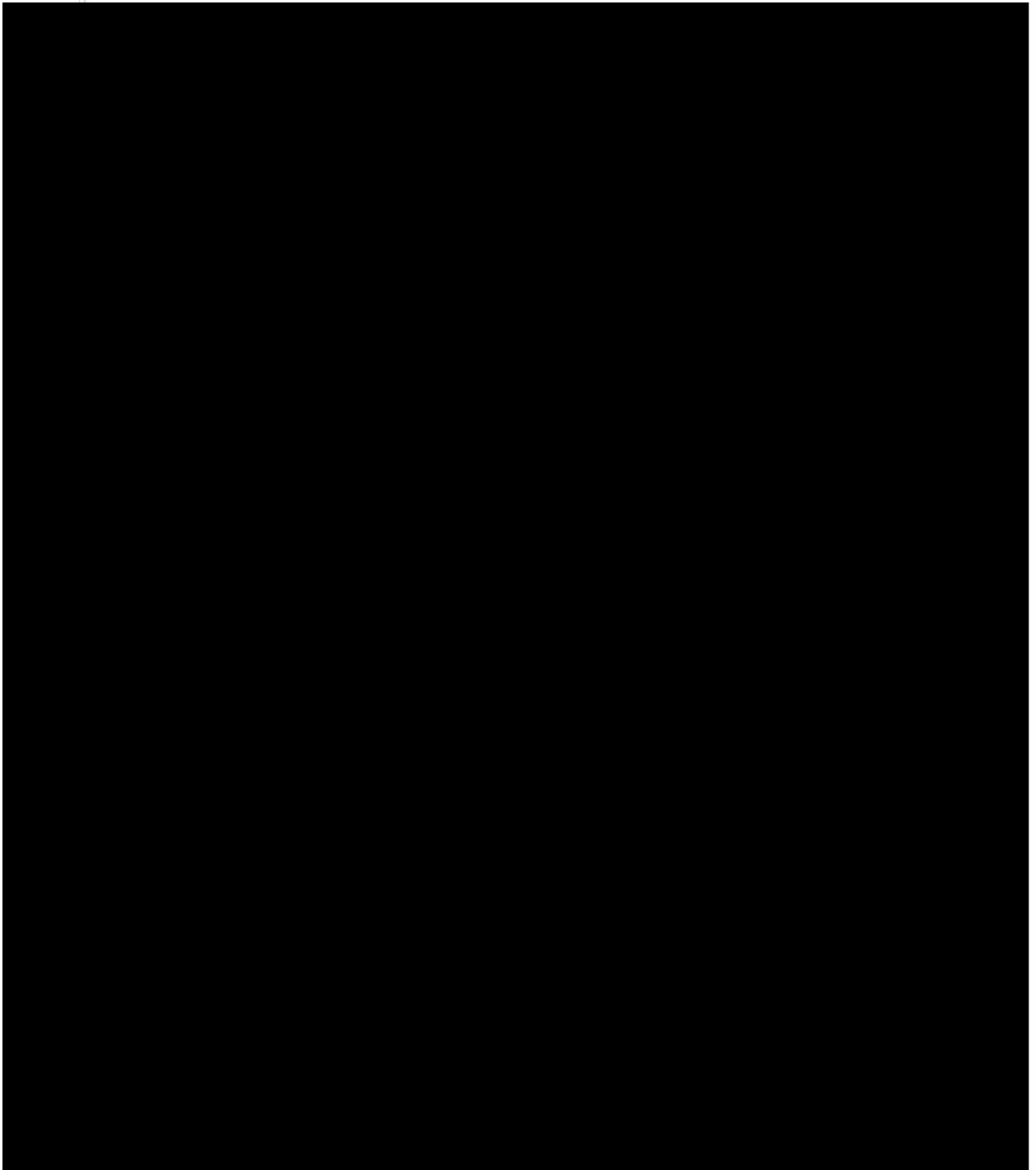
(c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

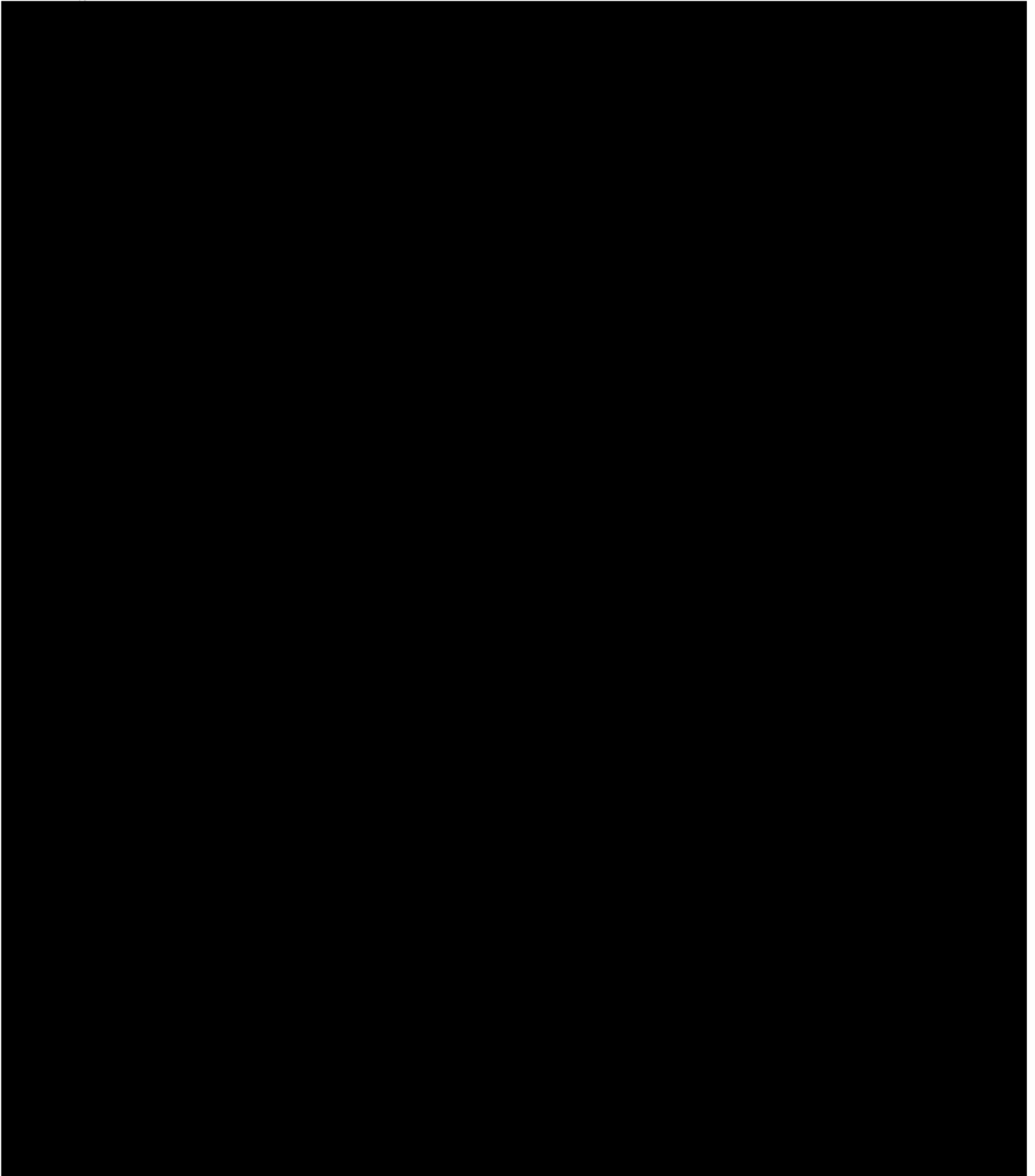
**PROBABLE CAUSE**



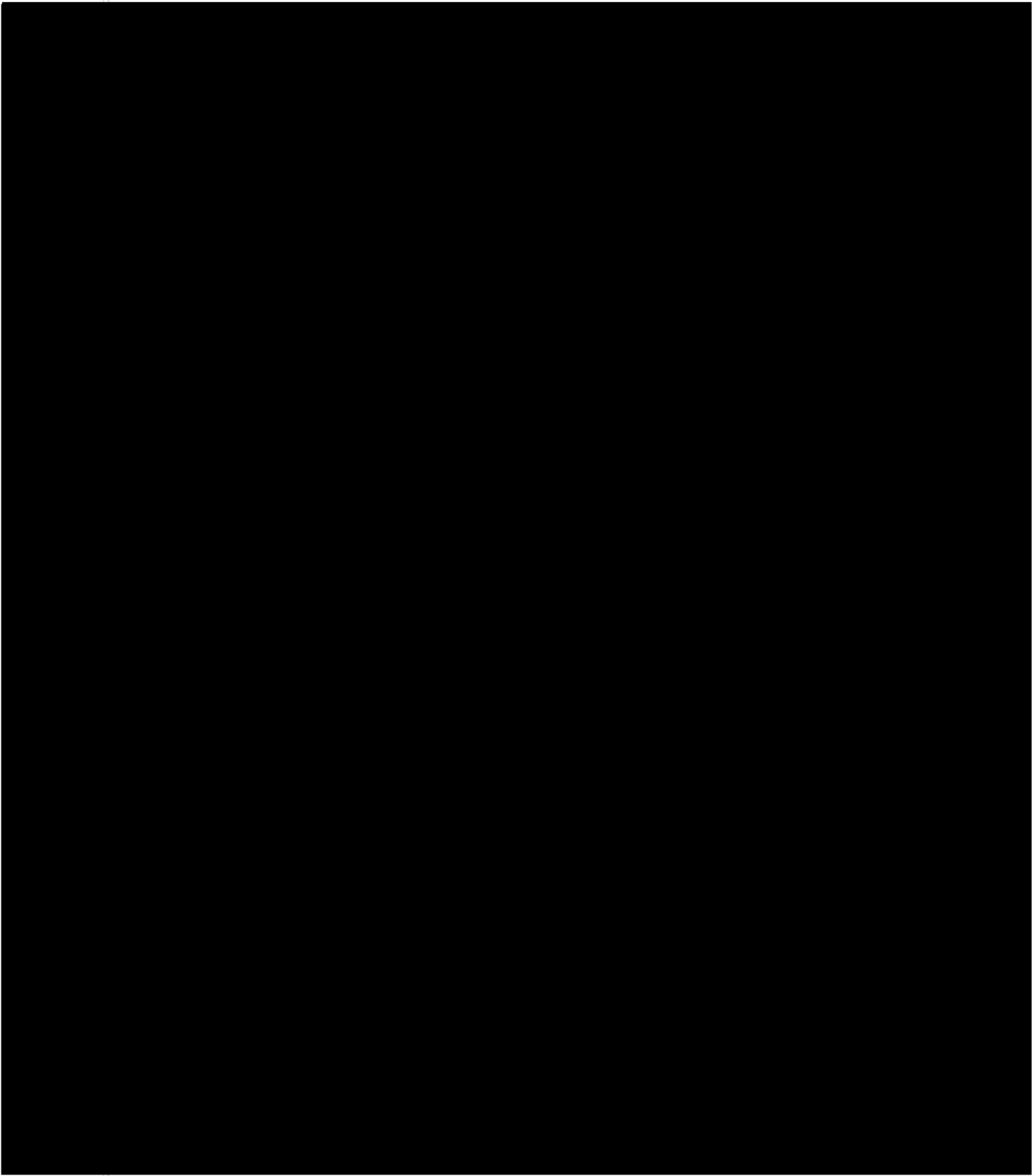


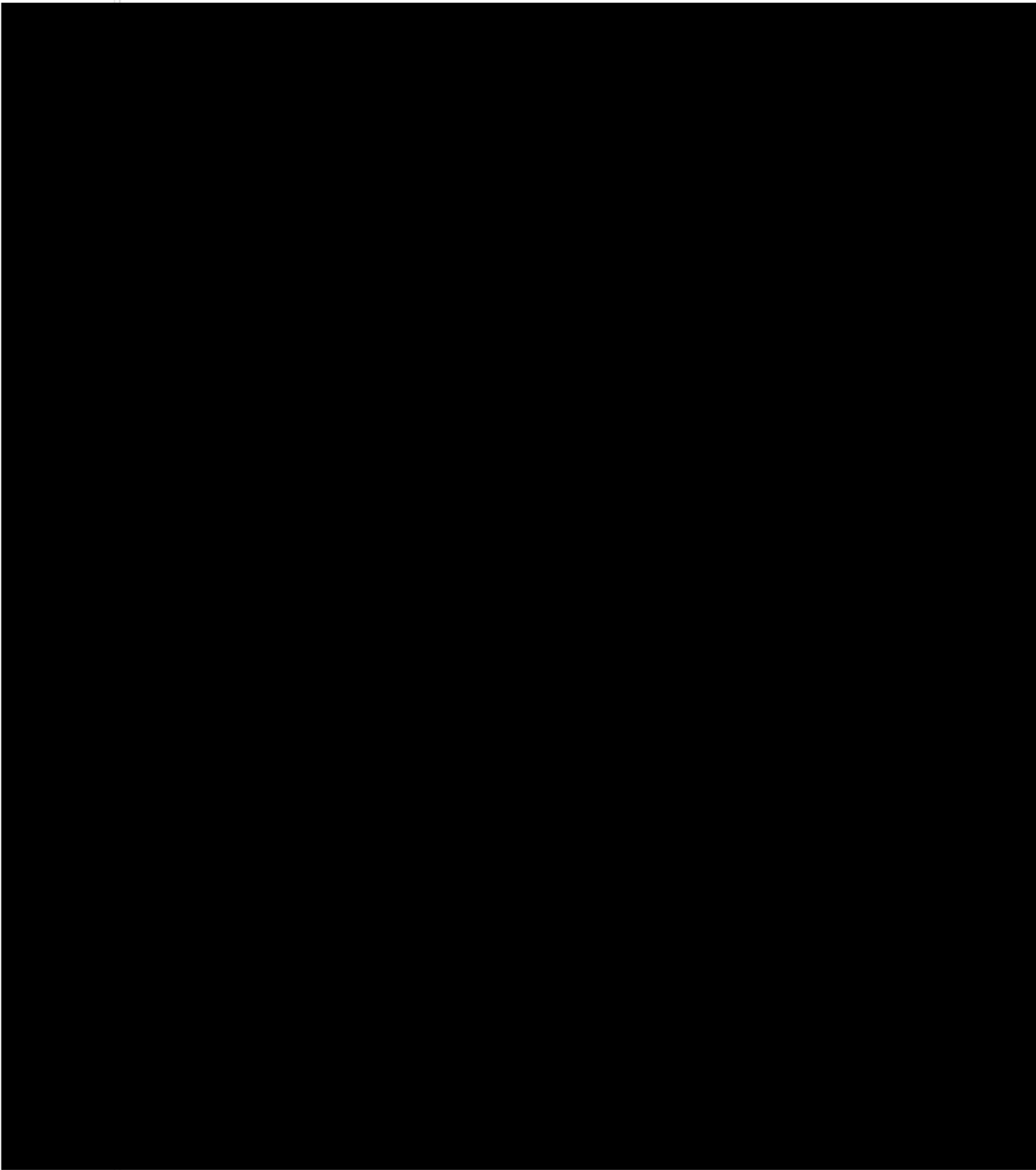












**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

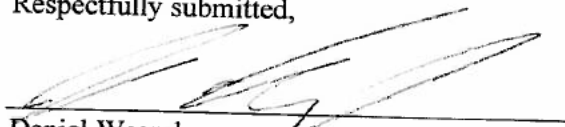
23. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require T-Mobile to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

**CONCLUSION**

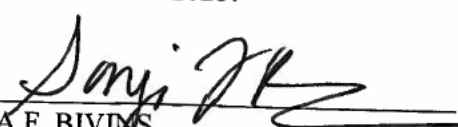
24. Based on the forgoing, I request that the Court issue the proposed search warrant.
25. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

26. The government will execute this warrant by serving the warrant on T-Mobile. Because the warrant will be served on T-Mobile, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

  
Daniel Wessel  
Postal Inspector  
US Postal Inspection Service

THE ABOVE AGENT HAS ATTESTED  
TO THIS AFFIDAVIT PURSUANT TO  
FED. R. CRIM. P. 4.1(b)(2)(B) THIS 11th  
DAY OF AUGUST 2023.

  
SONJA F. BIVINS  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with [REDACTED] that is stored at premises owned, maintained, controlled, or operated by T-Mobile, a wireless provider headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054.

**SEALED**

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by T-Mobile**

To the extent that the information described in Attachment A is within the possession, custody, or control of T-Mobile, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to T-Mobile or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), T-Mobile is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All voice mail, text, and multimedia messages **from October 27, 2021, to May 27, 2023** stored and presently contained in, or on behalf of the account or identifier;
- b. All existing printouts from original storage of all of the text messages described above;
- c. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used **from October 27, 2021, to May 27, 2023;**
- d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message **from October 27, 2021, to May 27, 2023;**
- e. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names,

addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

f. Detailed billing records, showing all billable calls including outgoing digits, **from October 27, 2021, to May 27, 2023;**

g. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number **from October 27, 2021, to May 27, 2023;**

h. Incoming and outgoing telephone numbers, **from October 27, 2021, to May 27, 2023;**

i. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;

j. All records pertaining to communications between T-Mobile and any person regarding the account or identifier, including contacts with support services and records of actions taken.

T-Mobile is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

## **II. Information to be seized by the government**

1. All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 1349 (fraud conspiracy), 1344 (bank fraud), 513(a) (possession of counterfeited or forged securities), 2314 (interstate transportation of counterfeited or forged securities), and 1028A (aggravated identity theft) involving [REDACTED]

[REDACTED] 1  
[REDACTED], and any other coconspirators, from **December 11, 2017, through and including June 27, 2023**, including but not limited to:

- a. Documents, identification cards, bank cards, credit applications, and any other documentation related to defrauding financial institutions and identity theft in furtherance of the scheme;
- b. Tools used to steal mail such as proprietary USPS mail storage keys (referred to as "Arrow Keys"), counterfeit USPS mail storage key, lock-picking kits, mail fishing devices, and the identities of USPS employees who may have provided to any of the above, or stolen U.S. mail in furtherance of the scheme;
- c. Checks and opened or unopened mail in furtherance of the scheme;
- d. Images of financial documents, letters, and other papers that are consistent with items stolen from the mail or the establishment of financial accounts using stolen/fictitious identities in furtherance of the scheme;
- e. Proceeds of crime such as cash, cashier's checks, money orders, pre-paid cards, account numbers, and other currencies/financial instruments;
- f. The identities of persons providing stolen/counterfeit/altered checks and personal information, as well as any communications with or about such persons;
- g. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;
- h. Evidence indicating the geographic location of the cellular device at times relevant to the investigation;



- i. Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;
- j. The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s).
- k. The identity of the person(s) who sent to and/or received communications from the cellular device about matters relating to the producing and depositing of counterfeit checks into financial institutions, solicitation of individuals with accounts at financial institutions, preparatory steps taken in furtherance of the scheme, and the theft of mail, including records that help reveal their whereabouts.